University of Bahrain IT College, CS Department **ITCS 412:** Cryptography Second Semester 2012/2013 Test II	St. ID : _____ Name : _____ Section : 1 (9:00) | 2 (12:00)

This exam consists of **6** pages. Duration: One hour

	Part 1	Part2	Part 3	Total
Maximum	10	15	15	40
Grade				

Part 1:

Answer the following questions by clearly circling the *most appropriate* answer

[1 point each]

1. If public-key encryption is used, encryption provides no confidence of sender since anyone potentially knows public-key. Is this statement true or false?
   a. True
   b. False

2. In SET protocol, the merchant can read both order and payment information. Is this statement true or false?
   a. True
   b. False

3. The SSL handshake protocol consists of how many phases
   a. Two phases
   b. Three phases
   c. Four phases
   d. Five phases

4. Which of the following techniques is **not** proposed for the distribution of public keys
   a. hybrid private-key distribution
   b. publicly available directory
   c. public-key authority
   d. public-key certificates

5. What is the main disadvantage of public-key authority for public key distribution.

    a. A user must appeal the authority for a public key for every other user it wishes to contact.
    b. Anyone can forge the public key request message
    c. The user can pretend to be another user and send a public key to another participant
    d. The timestamp may expire.

6. Which of the following is ***not*** true on a Certificate scheme:

    a. Only the CA can create and update certificates.
    b. Only the participant can sign certificates
    c. Any participant can read a certificate
    d. Any participant can verify that the certificate originated from the certificate authority (CA).

7. Which of the following is not correct about a hash function

    a. A hash function maps from a domain to a smaller range, typically many-to-one.
    b. Applications for hash function are error detection
    c. Provides strong message confidentiality
    d. Applications for hash function to store users passwords in a file
    e. If input to hash function is finite (pre-determined) is also called a compression function.

8. Digital signatures do provide the ability to,

    a. Verify author, date & time of signature.
    b. Authenticate message content
    c. Be verified by third parties to resolve disputes.
    d. A digital signature is analogous to the handwritten signature.
    e. All of the above

9. In SSL handshake phase two, the server sends server_key_exchange, certificate request, server_hello_done messages. Which of the messages is mandatory

    a. server_key_exchange
    b. certificate request
    c. server_hello_done
    d. none of the above

10. In RSA, select ***e*** such that ***e*** is relatively prime to ϕ(n). what does relatively prime means,

    a. *e* and ϕ(n) are multiplicative inverses modulo ϕ(n)
    b. *e* is a prime number modulo ϕ(n)
    c. *e* mod ϕ(n) = d
    d. *GCD*(e, ϕ(n)) = 1, i.e. the greatest common divisor between them is one

Part 2:

1. Answer the following: [2 points]

   i. Define: data origin authentication:

   ii. Propose a solution if Bob receives a message *m* from Alice and he wants to have Data origin authentication.

   iii. Define: Data integrity

   iv. Propose a solution if Bob receives a message *m* from Alice and he wants to have data integrity.

2. Answer the following: [4 points]

   i. Define Message Authentication Code (MAC)

   ii. If we have a hash function, how do we construct a MAC from it?

   iii. A digital signature is the same as a MAC?

   iv. Is it better to compute MAC before or after message encryption? why

1. What is the birthday problem? [1 points]

2. What is the role of the SSL Alert protocol? [1 points]

3. What is the role of the SSL Change cipher spec protocol? [1 points]

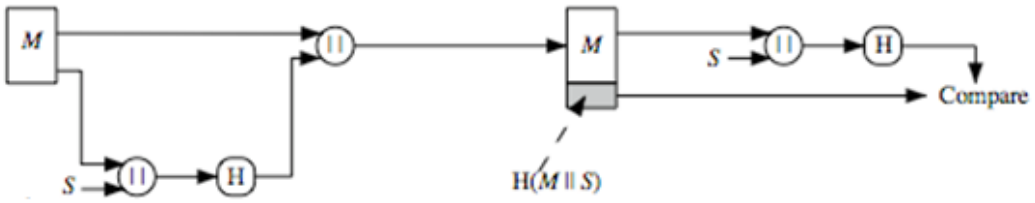
4. What is the purpose of the dual signature in SET protocol? [2 points]

5. In SET protocol, the merchant forwards to the payment Gateway (bank) encrypted blocks of related payment information sent by the cardholder. What do the encrypted blocks contain? and what type of verification the payment gateway performs from it? [4 points]

Part 3:

1. If Bob signed message m_1 and message m_2 using RSA, then the signature for message $m_1 m_2$ can be easily forged. Prove. [2 points]

2. Find a solution to countermeasure previous attack. [1 points]



3. The above figure shows the use of a hash function. The technique assumes that the two communicating parties share a common secret value S. Explain one advantage **or** one disadvantage of the above message authentication, if any. [2 points]

4. List three hash function requirements: [3 points]
   i. Variable input size: H can be applied to a block of data of any size
   ii. Efficiency: relatively easy to compute H(x)
   iii.
   iv.
   v.

5. How do we resist birthday attacks on hash functions? [1 points]

6. Suppose that Alice chooses for an RSA system the primes p = 23, and q = 17, and the public key e = 7. [4 points]

   (a) Encrypt the plaintext M = 15.

   (b) Determine the private key d.

7. What is wrong with the following: Alice chooses for an RSA system the primes p = 7, and q = 11, and the public key e = 5 to encrypt message M=88. [1 points]

8. What is wrong with the following: Alice chooses for an RSA system the primes p = 11, and q = 17, and the public key e = 8 to encrypt message M=90. [1 points]

The following question will be used to measure the CSPI(e)-5
"Understand the importance of IT security to an organization"

What are the drivers/barriers of organizational adoption of security practices? [5 points]

University of Bahrain IT College, CS Department **ITCS 412:** Cryptography First Semester 2012/2013 Test II	St. ID : _____ Name : _____ Section : 1 (9:00) | 2 (12:00)

Answer Sheet

Part 1:

Answer the following questions by clearly circling the *most appropriate* answer

[1 point each]

11. If public-key encryption is used, encryption provides no confidence of sender since anyone potentially knows public-key. Is this statement true or false?

    c. True
    d. False

12. In SET protocol, the merchant can read both order and payment information. Is this statement true or false?

    c. True
    d. False

13. The SSL handshake protocol consists of how many phases

    e. Two phases
    f. Three phases
    g. Four phases
    h. Five phases

14. Which of the following techniques is **not** proposed for the distribution of public keys

    e. hybrid private-key distribution
    f. publicly available directory
    g. public-key authority
    h. public-key certificates

15. What is the main disadvantage of public-key authority for public key distribution.

    e. A user must appeal the authority for a public key for every other user it wishes to contact.
    f. Anyone can forge the public key request message
    g. The user can pretend to be another user and send a public key to another participant
    h. The timestamp may expire.

16. Which of the following is ***not*** true on a Certificate scheme:

    e. Only the CA can create and update certificates.
    f. Only the participant can sign certificates
    g. Any participant can read a certificate
    h. Any participant can verify that the certificate originated from the certificate authority (CA).

17. Which of the following is not correct about a hash function

    f. A hash function maps from a domain to a smaller range, typically many-to-one.
    g. Applications for hash function are error detection
    h. Provides strong message confidentiality
    i. Applications for hash function to store users passwords in a file
    j. If input to hash function is finite (pre-determined) is also called a compression function.

18. Digital signatures do provide the ability to,

    f. Verify author, date & time of signature.
    g. Authenticate message content
    h. Be verified by third parties to resolve disputes.
    i. A digital signature is analogous to the handwritten signature.
    j. All of the above

19. In SSL handshake phase two, the server sends server_key_exchange, certificate request, server_hello_done messages. Which of the messages is mandatory

    e. server_key_exchange
    f. certificate request
    g. server_hello_done
    h. none of the above

20. In RSA, select ***e*** such that ***e*** is relatively prime to ϕ(n). what does relatively prime means,

    e. *e* and ϕ(n) are multiplicative inverses modulo ϕ(n)
    f. *e* is a prime number modulo ϕ(n)
    g. *e* mod ϕ(n) = d
    h. *GCD*(e, ϕ(n)) = 1, i.e. the greatest common divisor between them is one